

Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19

Angenommen am 21. April 2020

Versionsüberblick

Version 1.1	5. Mai 2020	geringfügige Änderungen
Version 1.0	21. April 2020	Annahme der Leitlinien

Inhalt

Der Europäische Datenschutzausschuss

gestützt auf Artikel 70 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, im Folgenden „DSGVO"),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum, insbesondere auf Anhang XI und Protokoll 37 in der durch den Beschluss Nr. 154/2018 des Gemeinsamen EWR-Ausschusses vom 6. Juli 2018 geänderten Fassung,[1]

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung

HAT FOLGENDE LEITLINIEN ANGENOMMEN:

1 EINFÜHRUNG UND KONTEXT

1 Regierungen und private Akteure fassen zur Bewältigung der COVID-19-Pandemie auch datengesteuerte Lösungen ins Auge, was zahlreiche Bedenken hinsichtlich des Datenschutzes aufwirft.

2 Der EDSA betont ausdrücklich, dass der Rechtsrahmen für den Datenschutz flexibel gestaltet wurde, sodass damit sowohl eine wirksame Eindämmung der Pandemie als auch der Schutz der Menschenrechte und Grundfreiheiten erreicht werden können.

3 Der EDSA ist fest davon überzeugt, dass der Schutz der Daten bei der Verarbeitung personenbezogener Daten zur Bewältigung der COVID-19-Pandemie unabdingbar ist, um Vertrauen aufzubauen und die Voraussetzungen für die Akzeptanz diesbezüglicher Maßnahmen in der Gesellschaft zu schaffen, sodass deren Wirksamkeit gewährleistet ist. Da das Virus keine Grenzen kennt, sollte als Reaktion auf die aktuelle Krise vorzugsweise ein gemeinsamer europäischer Ansatz ausgearbeitet oder zumindest ein interoperabler Rahmen geschaffen werden.

4 Der EDSA ist allgemein der Ansicht, dass Daten und Technologien, die zur Bekämpfung von COVID-19 verwendet werden, Individuen zu eigenem Handeln befähigen sollten und nicht zu deren Kontrolle, Stigmatisierung oder Repression eingesetzt werden sollten.. Daten und Technologien können sich zwar als wichtige Instrumente erweisen, sind jedoch als solche beschränkt und können somit lediglich die Wirksamkeit weiterer Maßnahmen im Bereich der öffentlichen Gesundheit steigern. Alle Maßnahmen, die von den Mitgliedstaaten oder den EU-Organen zur Bekämpfung von COVID-19 ergriffen werden und die Verarbeitung personenbezogener Daten beinhalten, müssen den allgemeinen Grundsätzen der Wirksamkeit, Notwendigkeit und Verhältnismäßigkeit entsprechen.

5 Diese Leitlinien verdeutlichen die Bedingungen und Grundsätze für die verhältnismäßige Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung für zwei konkrete Anwendungen:

---

1 Soweit in diesen Empfehlungen auf „Mitgliedstaaten" Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten" zu verstehen.

- die Verwendung von Standortdaten zur Unterstützung der Reaktion auf die Pandemie durch die Modellierung der Verbreitung des Virus, sodass die Wirksamkeit der Beschränkungsmaßnahmen insgesamt beurteilt werden kann;
- die Kontaktnachverfolgung mit dem Ziel, Einzelpersonen darüber zu informieren, dass sie sich in unmittelbarer Nähe zu einer Person aufgehalten haben, die zu einem späteren Zeitpunkt als Träger des Virus bestätigt wurde, um so die Infektionsketten so früh wie möglich zu unterbrechen.

6 Wie wirksam Apps zur Kontaktnachverfolgung bei der Bewältigung der Pandemie sind, hängt von vielen Faktoren ab (z. B. dem Prozentsatz der Personen, die die Apps installieren müssten, der Festlegung eines „Kontakts“ hinsichtlich der Nähe und der Dauer). Zur Bekämpfung der Pandemie müssen solche Apps überdies in eine umfassende Strategie für die öffentliche Gesundheit eingebettet werden, unter anderem mit Tests und einer anschließenden manuellen Kontaktnachverfolgung, um Gewissheit zu erlangen. Ihre Einführung sollte von unterstützenden Maßnahmen flankiert werden, um sicherzustellen, dass die den Nutzern zur Verfügung gestellten Informationen kontextbezogen sind und Warnmeldungen für das öffentliche Gesundheitswesen von Nutzen sein können. Andernfalls könnten diese Apps ihre Wirkung nicht voll entfalten.

7 Der EDSA betont, dass die DSGVO und die Richtlinie 2002/58/EG (im Folgenden die „Richtlinie“) beide konkrete Bestimmungen enthalten, die die Verwendung anonymisierter oder personenbezogener Daten zur Unterstützung der Behörden und anderer Akteure auf nationaler und EU-Ebene bei der Überwachung und Eindämmung der Ausbreitung des SARS-CoV-2-Virus ermöglichen.[2]

8 Diesbezüglich hat der EDSA bereits Stellung zu der Tatsache genommen, dass Apps zur Kontaktnachverfolgung auf freiwilliger Basis verwendet werden sollten und nicht auf der Verfolgung individueller Bewegungsdaten, sondern auf Informationen über die räumliche Nähe von Nutzern basieren sollten.[3]

[2] Siehe jüngste Stellungnahme des EDSA zum COVID-19-Ausbruch.
[3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 VERWENDUNG VON STANDORTDATEN

2.1 Quellen für Standortdaten

9 Für die Modellierung der Ausbreitung des Virus und der generellen Wirksamkeit der Ausgangsbeschränkungen stehen zwei wesentliche Quellen für Standortdaten zur Verfügung:

- Standortdaten, die von Anbietern elektronischer Kommunikationsdienste (wie Mobilfunkbetreibern) bei der Erbringung ihrer Dienste erhoben werden, und
- Standortdaten, die von Anbietern von Diensten der Informationsgesellschaft, für deren Funktion diese Daten erforderlich sind, erhoben werden (z. B. Navigation, Beförderungsdienste usw.).

10 Der EDSA erinnert daran, dass die von Anbietern elektronischer Kommunikationsdienste erhobenen Standortdaten[4] nur im Rahmen von Artikel 6 und 9 der Richtlinie verarbeitet werden dürfen. Das heißt, dass diese Daten nur an Behörden oder andere Dritte übermittelt werden dürfen, wenn sie vom Anbieter anonymisiert wurden oder wenn der Nutzer vorher seine Einwilligung zur Übermittlung von Daten erteilt hat, die den geografischen Standort des Endgeräts eines Nutzers angeben, jedoch keine Verkehrsdaten sind.[5]

11 Was Informationen, einschließlich Standortdaten anbelangt, die direkt über das Endgerät erhoben werden, gilt Artikel 5 Absatz 3 der Richtlinie. Die Speicherung von Informationen im Gerät des Nutzers oder der Zugang zu bereits darin gespeicherten Informationen ist daher nur dann zulässig, wenn (i) der Nutzer seine Einwilligung[6] erteilt hat oder (ii) die Speicherung und/oder der Zugang unbedingt erforderlich ist, um einen vom Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft zur Verfügung zu stellen.

12 Die in der Richtlinie vorgesehenen Beschränkungen der Rechte und Pflichten nach Artikel 15 sind möglich, sofern sie für bestimmte Ziele in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig sind.[7]

13 Was die Weiterverwendung von Standortdaten anbelangt, die von Diensten der Informationsgesellschaft zu Modellierungszwecken (z. B. durch das Betriebssystem oder eine vorher installierte App) erhoben werden, so müssen weitere Bedingungen erfüllt sein. Wenn Informationen im Einklang mit Artikel 5 Absatz 3 der Richtlinie erhoben wurden, dürfen diese nur mit zusätzlicher Einwilligung der betroffenen Person oder auf der Grundlage einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 DSGVO genannten Ziele darstellt, weiterverarbeitet werden.[8]

2.2 Besondere Betrachtung zur Verwendung von anonymisierten Standortdaten

14 Der EDSA betont, dass bei der Verwendung von Standortdaten vorrangig anonymisierte Daten statt personenbezogene Daten verarbeitet werden sollten.

15 Unter Anonymisierung ist die Verwendung einer Reihe von Techniken zu verstehen, sodass diese Daten nur mit einem unverhältnismäßig hohen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Diese Verhältnismäßigkeitsprüfung („reasonability test“) muss sowohl objektive Aspekte (Zeit, technische Mittel) als auch kontextuelle Elemente berücksichtigen, die von Fall zu Fall variieren können (Seltenheit eines Phänomens, einschließlich Bevölkerungsdichte, Art und

[4] Siehe Artikel 2 Buchstabe c der Richtlinie.
[5] Siehe Artikel 6 und 9 der Richtlinie.
[6] Der Begriff der Einwilligung im Sinne der Richtlinie entspricht dem Begriff der Einwilligung nach der DSGVO und muss alle Anforderungen an die Einwilligung nach Artikel 4 Absatz 11 und Artikel 7 DSGVO erfüllen.
[7] Zur Auslegung von Artikel 15 der Richtlinie siehe auch das Urteil des EuGH vom 29. Januar 2008 in der Rechtssache C-275/06, Productores de Música de España (Promusicae)/Telefónica de España SAU.
[8] Siehe Abschnitt 1.5.3 der Leitlinien 1/2020 über die Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen.

Umfang der Daten). Wenn die Daten diese Prüfung nicht bestehen, so wurden sie nicht anonymisiert und fallen daher in den Anwendungsbereich der DSGVO.

16 Für die Bewertung der Zuverlässigkeit des Anonymisierungsprozesses sind folgende drei Kriterien maßgeblich: (i) die datenbasierte Isolierung einer Einzelperson aus einer größeren Gruppe, (ii) die Verknüpfbarkeit zweier sich auf ein- und dieselbe Person beziehender Datensätze und (iii) die mit hoher Genauigkeit erfolgende Herleitung bisher unbekannter Informationen über eine Einzelperson.

17 Das Konzept der Anonymisierung ist anfällig für Missverständnisse und wird oft mit Pseudonymisierung verwechselt. Während die Anonymisierung eine uneingeschränkte Verwendung der Daten erlaubt, fallen pseudonymisierte Daten nach wie vor in den Anwendungsbereich der DSGVO.

18 Es gibt viele Möglichkeiten für eine wirksame Anonymisierung[9], die allerdings mit einem Vorbehalt behaftet sind. Die Daten als solche können nicht anonymisiert werden, d. h. nur Datensätze als Ganzes können anonymisiert werden. In diesem Sinne kann jedweder Eingriff an einem einzigen Datenmuster (durch Verschlüsselung oder andere mathematische Transformationen) im besten Falle nur als Pseudonymisierung angesehen werden.

19 Zu Anonymisierungsverfahren und Deanonymisierungsangriffen wird aktiv geforscht. Für jeden Verantwortlichen, welcher Anonymisierungslösungen implementiert, ist es entscheidend, jüngste Entwicklungen in diesem Bereich zu beobachten, insbesondere in Bezug auf Standortdaten (von Telekommunikationsbetreibern und/oder Diensten der Informationsgesellschaft), die bekanntlich schwer zu anonymisieren sind.

20 Tatsächlich hat ein großes Forschungsinstitut festgestellt[10], dass *vermeintlich anonymisierte Standortdaten* wahrscheinlich gar nicht anonymisiert wurden. Mobilitätsspuren von Einzelpersonen sind naturgemäß stark korreliert und einzigartig. Daher können sie unter bestimmten Umständen für Deanonymisierungsverfahren anfällig sein.

21 Ein einzelnes Datenmuster zum Standort-Tracking einer Einzelperson über einen signifikanten Zeitraum hinweg kann nicht vollständig anonymisiert werden. Dies gilt unter Umständen auch dann, wenn die Genauigkeit der aufgezeichneten geografischen Koordinaten nicht ausreichend verringert wird oder, wenn einzelne Elemente der Spur entfernt werden und selbst dann, wenn nur der Standort der Orte, wo sich die betroffene Person eine beträchtliche Zeit aufhält, erhoben wird. Gleiches trifft für schlecht aggregierte Standortdaten zu.

22 Standortdaten müssen zwecks Anonymisierung mit großer Sorgfalt verarbeitet werden, um die Verhältnismäßigkeitsprüfung (reasonability test) zu bestehen. Daher sind bei einer solchen Verarbeitung ganze Standortdatensätze sowie die Verarbeitung von Daten einer relativ großen Zahl von Einzelpersonen unter Verwendung zuverlässiger Anonymisierungstechniken zu berücksichtigen, sofern diese angemessen und wirksam implementiert werden.

23 Zu guter Letzt wird angesichts der Komplexität von Anonymisierungsprozessen nachdrücklich Transparenz in Bezug auf die Anonymisierungsmethode empfohlen.

---

[9] Vgl. de Montjoye et al., 2018, „On the privacy-conscientious use of mobile phone data".
[10] Vgl. de Montjoye et al., 2013, „Unique in the Crowd: The privacy bounds of human mobility" und Pyrgelis et al., 2017, „Knock, Who's There? Membership Inference on Aggregate Location Data".

3 APPS ZUR KONTAKTNACHVERFOLGUNG

3.1 Allgemeine rechtliche Prüfung

24 Die systematische und umfassende Überwachung des Standortes und/oder der Kontakte zwischen natürlichen Personen ist ein schwerwiegender Eingriff in deren Privatsphäre. Dieser ist nur dann legitim, wenn der Nutzer die App für jeden der vorgesehenen Zwecke freiwillig verwendet. Im Umkehrschluss bedeutet dies, dass Personen, die solche Apps nicht nutzen möchten oder können, keine Nachteile entstehen dürfen.

25 Um die Rechenschaftspflicht zu gewährleisten, sollte der Verantwortliche für eine Kontaktnachverfolgungs-App klar definiert werden. Der EDSA ist der Auffassung, dass die nationalen Gesundheitsbehörden als Verantwortliche[11] für derartige Apps fungieren könnten; andere Verantwortliche könnten ebenfalls in Erwägung gezogen werden. Wenn an der Einführung von Apps zur Kontaktnachverfolgung verschiedene Akteure beteiligt sind, so sind deren Funktionen und Zuständigkeiten von Anfang an klar festzulegen und den Nutzern zu erklären.

26 Darüber hinaus müssen die Zwecke mit Blick auf den Grundsatz der Zweckbindung ausreichend konkret sein, damit eine weitere Verarbeitung zu Zwecken, die nicht mit der Bewältigung der COVID-19-Gesundheitskrise zusammenhängen (z. B. kommerzielle- oder Strafverfolgungszwecke), ausgeschlossen ist. Sobald das Ziel klar definiert ist, muss gewährleistet werden, dass die Nutzung von personenbezogenen Daten geeignet, erforderlich und angemessen ist.

27 Bei einer App zur Kontaktnachverfolgung sollten die Grundsätze der Datenminimierung sowie des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen eingehend berücksichtigt werden:

- Für Kontaktnachverfolgungs-Apps ist eine Standortortung der einzelnen Nutzer nicht erforderlich. Stattdessen sollten Begegnungsdaten verwendet werden.
- Da Apps zur Kontaktnachverfolgung ohne eine direkte Identifizierung von Einzelpersonen funktionieren können, sollten geeignete Maßnahmen getroffen werden, um eine Deanonymisierung zu verhindern.
- Die erhobenen Informationen sollten im Endgerät des Nutzers verbleiben und lediglich relevante Informationen sollten, sofern absolut notwendig, erhoben werden.

28 Hinsichtlich der Rechtmäßigkeit der Verarbeitung stellt der EDSA fest, dass Apps zur Kontaktnachverfolgung die Speicherung und/oder den Zugang zu Informationen, die bereits im Endgerät gespeichert sind, voraussetzen. Diese Vorgänge unterliegen Artikel 5 Absatz 3 der Richtlinie. Wenn diese Vorgänge unbedingt erforderlich sind, damit der Anbieter der App den vom Nutzer ausdrücklich angeforderten Dienst anbieten kann, ist die Einwilligung des Nutzers für die Verarbeitung nicht erforderlich. Für Vorgänge, die nicht zwingend erforderlich sind, ist die Einwilligung des Nutzers einzuholen.

29 Darüber hinaus weist der EDSA darauf hin, dass allein die Tatsache, dass Apps zur Kontaktnachverfolgung freiwillig genutzt werden, nicht notwendigerweise bedeutet, dass die Verarbeitung personenbezogener Daten auf Basis einer Einwilligung erfolgen wird. Wenn Behörden einen Dienst auf der Grundlage eines gesetzlichen Auftrags im Einklang mit den gesetzlichen Anforderungen erbringen, so stellt die Verarbeitung für die Wahrnehmung einer Aufgabe im öffentlichen Interesse die relevanteste Rechtsgrundlage für die Verarbeitung dar (d. h. Artikel 6 Absatz 1 Buchstabe e DSGVO).

30 In Artikel 6 Absatz 3 DSGVO ist klar dargelegt, dass die Grundlage für die Verarbeitung nach Artikel 6 Absatz 1 Buchstabe e durch das Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, festgelegt wird. Der Zweck der Verarbeitung muss in dieser

[11] Siehe Mitteilung der Kommission „Leitlinien zum Datenschutz bei Mobil-Apps zur Unterstützung der Bekämpfung der COVID-19-Pandemie", Brüssel, 16.4.2020 C(2020) 2523 final.

Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.[12]

31 Die Rechtsgrundlage oder die Rechtsvorschrift, die als rechtmäßige Grundlage für die Verwendung von Kontaktnachverfolgungs-Apps dient, sollte jedoch wirksame Garantien enthalten, darunter einen Verweis auf die freiwillige Nutzung der Anwendung. Eine klare Beschreibung des Zwecks und die eindeutige Zweckbindung hinsichtlich einer weiteren Verarbeitung von personenbezogenen Daten sowie die/der beteiligte/n Verantwortliche/n sollten eindeutig festgelegt werden. Die Datenkategorien sowie die Einrichtungen (und Zwecke), für die personenbezogene Daten offengelegt werden können, sollten ebenfalls festgelegt werden. Je nach Umfang der Beeinträchtigung sollten zusätzliche Garantien eingeführt werden, die der Art, dem Umfang und den Zwecken der Verarbeitung Rechnung tragen. Schließlich empfiehlt der EDSA auch, baldmöglichst Kriterien festzulegen, nach denen sich bestimmen lässt, wann die App abgeschafft werden soll und welche Stelle für diese Entscheidung zuständig und verantwortlich ist.

32 Basiert die Datenverarbeitung auf einer anderen Rechtsgrundlage – wie einer Einwilligung nach Artikel 6 Absatz 1 Buchstabe a – muss der Verantwortliche sicherstellen, dass die strengen Anforderungen, die für diese Rechtsgrundlage gelten, erfüllt werden.[13]

33 Darüber hinaus könnte eine App zur Bekämpfung der COVID-19-Pandemie zur Erhebung von Gesundheitsdaten führen (zum Beispiel zum Status einer infizierten Person). Die Verarbeitung dieser Daten ist zulässig, wenn die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit notwendig ist und die Bedingungen nach Artikel 9 Absatz 2 Buchstabe i DSGVO[14] oder für die Zwecke der Gesundheitsdienste nach Artikel 9 Absatz 2 Buchstabe h DSGVO[15] erfüllt sind. Je nach Rechtsgrundlage könnte die Verarbeitung auch auf die ausdrückliche Einwilligung nach Artikel 9 Absatz 2 Buchstabe a DSGVO gestützt werden.

34 Im Einklang mit dem ursprünglichen Zweck ist nach Artikel 9 Absatz 2 Buchstabe j DSGVO die Verarbeitung von Gesundheitsdaten auch zulässig, wenn sie für wissenschaftliche Forschungszwecke oder für statistische Zwecke erforderlich ist.

35 Die derzeitige Gesundheitskrise sollte nicht als Gelegenheit genutzt werden, unverhältnismäßige Verpflichtungen zur Vorratsdatenspeicherung einzuführen. Bei einer Speicherbegrenzung sollte den tatsächlichen Bedürfnissen und der medizinischen Relevanz Rechnung getragen werden (dazu können epidemiologisch motivierte Erwägungen wie die Inkubationszeit usw. gehören). Personenbezogene Daten sollten nur für die Dauer der COVID-19-Krise gespeichert werden. Danach sollten sämtliche personenbezogenen Daten grundsätzlich gelöscht oder anonymisiert werden.

36 Nach dem Verständnis des EDSA können solche Apps die manuelle Kontaktnachverfolgung durch geeignetes Gesundheitspersonal, das prüfen kann, ob enge Kontakte wahrscheinlich zu einer Virusübertragung führen oder nicht (z. B. beim Kontakt mit einer Person, die durch eine geeignete Ausrüstung geschützt - Kassierer usw. – oder eben nicht geschützt ist), nicht ersetzen, sondern nur unterstützen. Der EDSA betont, dass von der Kontaktnachverfolgungs-App implementierte Verfahren und Prozesse, einschließlich entsprechender Algorithmen, unter strenger Aufsicht von qualifiziertem Personal ablaufen sollten, um das Auftreten falscher positiver und negativer Ergebnisse einzuschränken. Insbesondere sollten Empfehlungen für

---

[12] Siehe Erwägungsgrund 41.

[13] Verantwortliche (insbesondere Behörden) müssen besonders darauf achten, dass die Einwilligung nicht als freiwillig anzusehen ist, wenn Bürger keine echte Wahl haben, ihre Einwilligung zu verweigern oder zu widerrufen, ohne einen Nachteil zu erleiden.

[14] Die Verarbeitung muss auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats erfolgen, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses vorsieht.

[15] Siehe Artikel 9 Absatz 2 Buchstabe h DSGVO.

den Nutzer, wie weiter zu verfahren ist, nicht ausschließlich auf eine automatisierte Verarbeitung gestützt erfolgen.

37 Algorithmen müssen überprüfbar sein und regelmäßig von unabhängigen Sachverständigen geprüft werden, um zu gewährleisten, dass sie den Grundsätzen der Fairness, Rechenschaftspflicht und allgemeiner den gesetzlichen Anforderungen genügen. Der Quellcode der App sollte öffentlich und so der größtmöglichen Kontrolle zugänglich gemacht werden.

38 Falsche positive Ergebnisse werden bis zu einem gewissen Maße immer auftreten. Da die Feststellung des Infektionsrisikos wahrscheinlich große Auswirkungen auf Einzelpersonen haben kann (wie die Selbstisolierung bis zur negativen Testung), muss es möglich sein, Daten zu korrigieren und/oder Ergebnisse im Anschluss zu analysieren. Dies sollte natürlich nur für Fälle und Implementierungen gelten, wo Daten so verarbeitet und/oder gespeichert werden, dass solche Korrekturen technisch möglich sind und mit den vorgenannten gegenteiligen Wirkungen zu rechnen ist.

39 Schließlich ist der EDSA der Auffassung, dass eine Datenschutz-Folgenabschätzung (DSFA) vor der Einführung eines solchen Instruments ausgeführt werden muss, da die Verarbeitung als mit einem hohen Risiko (Gesundheitsdaten, voraussichtliche flächendeckende Einführung, systematische Überwachung, Einsatz neuer technologischer Lösungen) behaftet eingestuft wird.[16] Der EDSA empfiehlt nachdrücklich, dass Datenschutz-Folgenabschätzungen veröffentlich werden.

3.2 Empfehlungen und Funktionsanforderungen

40 Nach dem Grundsatz der Datenminimierung, wozu auch Maßnahmen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen[17] gehören, sollten die verarbeiteten Daten auf das absolute Mindestmaß reduziert werden. Mit der App dürfen keine zusammenhanglosen oder nicht benötigten Informationen erhoben werden, zu denen u. a. Personenstand, Kommunikationskennungen, Geräteordner, Nachrichten, Anrufprotokolle, Standortdaten und Gerätekennungen gehören können.

41 Die von einer App gesendeten Daten dürfen nur einige eindeutige, pseudonymisierte Kennungen enthalten, die von der App generiert werden und für sie spezifisch sind. Diese Kennungen müssen regelmäßig und so oft erneuert werden, wie es mit dem Zweck vereinbar ist, die Ausbreitung des Virus einzudämmen, und ausreicht, um das Risiko der Identifizierung und der physischen Nachverfolgung von Personen zu begrenzen.

42 Implementierungen für die Kontaktnachverfolgung können einem zentralen oder dezentralen Ansatz folgen.[18] Sofern angemessene Sicherheitsmaßnahmen getroffen werden, können beide Optionen mit den ihnen eigenen Vor- und Nachteilen in Betracht gezogen werden. In der Konzeptionsphase einer App sollten daher stets beide Optionen eingehend unter sorgfältiger Abwägung ihrer Auswirkungen auf den Datenschutz/die Privatsphäre und ihre möglichen Auswirkungen auf die Rechte des Einzelnen geprüft werden.

43 Jeder am Kontaktnachverfolgungssystem beteiligte Server darf nur auf freiwillige Veranlassung des Nutzers hin die Kontakthistorie oder die pseudonymisierten Kennungen dieses Nutzers erfassen, dessen Infektion von den Gesundheitsbehörden ordnungsgemäß festgestellt wurde. Alternativ dazu darf der Server eine Liste pseudonymisierter Kennungen infizierter Nutzer oder deren Kontakthistorie nur so lange aufbewahren, bis potenziell

---

[16] Siehe WP 29 Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) (angenommen vom EDSA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung (EU) 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“.

[17] Siehe EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (EDSA-Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen).

[18] Eine dezentrale Lösung entspricht im Allgemeinen eher dem Grundsatz der Datenminimierung.

infizierte Nutzer über ihre Exposition informiert worden sind; er darf nicht versuchen, diese Nutzer zu identifizieren.

44 Die Einführung einer umfassenden Methode zur Nachverfolgung von Kontakten, die sowohl Anwendungen als auch eine manuelle Nachverfolgung beinhaltet, kann in einigen Fällen die Verarbeitung zusätzlicher Informationen erforderlich machen. Diese zusätzlichen Informationen sollten in diesem Fall im Endgerät des Nutzers verbleiben und nur verarbeitet werden, wenn dies unbedingt erforderlich ist und der Nutzer vorher ausdrücklich in die Verarbeitung eingewilligt hat.

45 Zur Sicherung der in Servern und Apps gespeicherten Daten und der Daten, die zwischen Apps und dem Fernserver ausgetauscht werden, müssen kryptografische Techniken nach Stand der Technik eingesetzt werden. Zwischen der App und dem Server muss zudem eine gegenseitige Authentifizierung erfolgen.

46 Die Meldung von SARS-CoV2-infizierten Nutzern über die App muss einer ordnungsgemäßen Autorisierung unterliegen, z. B. durch einen Einmalcode, der an eine pseudonymisierte Identität der infizierten Person gekoppelt und mit einer Testeinrichtung oder einer Gesundheitsfachkraft verbunden ist. Kann eine Bestätigung nicht auf sichere Weise erlangt werden, sollte keine Datenverarbeitung stattfinden, die von der Gültigkeit des Nutzerstatus ausgeht.

47 Der Verantwortliche muss in Zusammenarbeit mit den Behörden klar und konkret über den Link zum Herunterladen der amtlichen nationalen App zur Kontaktnachverfolgung informieren, um das Risiko zu mindern, dass eine App Dritter genutzt wird.

4 FAZIT

48 Die Welt ist mit einer schweren Krise im Bereich der öffentlichen Gesundheit konfrontiert, die entschlossenes Handeln erfordert, das über diese Notlage hinaus Folgen haben wird. Automatisierte Datenverarbeitung und digitale Technologien können bei der Bekämpfung von COVID-19 eine zentrale Rolle spielen. Angesichts eines möglichen „Ratchet-Effekts“ ist jedoch Vorsicht geboten. Es liegt in unserer Verantwortung, dafür zu sorgen, dass jede unter diesen außergewöhnlichen Umständen ergriffene Maßnahme notwendig, zeitlich begrenzt und von minimaler Tragweite ist und einer regelmäßigen, konkreten Überprüfung sowie einer wissenschaftlichen Bewertung unterliegt.

49 Der Europäische Datenschutzausschuss betont, dass es nicht dazu kommen dürfe, zwischen einer wirksamen Reaktion auf die derzeitige Krise und dem Schutz unserer Grundrechte wählen zu müssen: Wir können beides erreichen; nicht zuletzt können Datenschutzgrundsätze eine sehr wichtige Rolle bei der Bekämpfung des Virus spielen. Das europäische Datenschutzrecht ermöglicht die verantwortungsvolle Nutzung personenbezogener Daten für Zwecke des Gesundheitsmanagements und stellt gleichzeitig sicher, dass die Rechte und Freiheiten des Einzelnen dabei nicht beeinträchtigt werden.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)

ANHANG -- KONTAKTNACHVERFOLGUNGS-APPS
ORIENTIERUNGSHILFE FÜR DIE ANALYSE EINSCHLÄGIGER APPS

0. Hinweis

Die folgenden Empfehlungen sind weder präskriptiv noch erschöpfend. Ihr einziger Zweck besteht darin, für die Entwicklung und Implementierung von Anwendungen zur Kontaktnachverfolgung allgemeine Empfehlungen zur Verfügung zu stellen. Es können auch andere als die hier beschriebenen Lösungen rechtmäßig sein und genutzt werden, solange sie den einschlägigen rechtlichen Vorgaben (d. h. der DSGVO und der Richtlinie) entsprechen.

Es sei ferner darauf hingewiesen, dass diese Empfehlungen allgemein gehalten sind. Die hier skizzierten Empfehlungen und Verpflichtungen dürfen daher nicht als erschöpfend betrachtet werden. Jede Bewertung muss von Fall zu Fall erfolgen. Für bestimmte Anwendungen können zusätzliche Maßnahmen erforderlich sein, die nicht in diesen Leitlinien enthalten sind.

1. Zusammenfassung

In vielen Mitgliedstaaten wird die Verwendung von *Kontaktnachverfolgungs*-Apps erwogen, damit Bürgerinnen und Bürger feststellen können, ob sie mit einer mit SARS-CoV-2-infizierten Person in Kontakt waren.

Es ist noch offen, unter welchen Bedingungen solche Apps einen effektiven Beitrag zum Umgang mit der Pandemie leisten können. Diese Bedingungen müssten vor Einführung einer solchen App definiert werden. Dennoch ist es wichtig, Empfehlungen zur Verfügung zu stellen, mit denen den Entwicklerteams einschlägige Informationen erhalten, damit der Schutz personenbezogener Daten bereits in der frühen Entwurfsphase gewährleistet werden kann.

Die vorliegenden Empfehlungen sind allgemein gehalten. Die hier skizzierten Empfehlungen und Verpflichtungen dürfen daher nicht als erschöpfend betrachtet werden. Jede Bewertung muss von Fall zu Fall erfolgen. Für bestimmte Anwendungen können zusätzliche Maßnahmen erforderlich sein, die nicht in diesen Empfehlungen enthalten sind. Die folgenden Empfehlungen sollen eine allgemeine Orientierung für die Entwicklung und Implementierung von Kontaktnachverfolgungs-Apps bieten.

Einige Kriterien gehen unter Umständen über die strengen Anforderungen des Datenschutzrechts hinaus. Sie sollen ein Höchstmaß an Transparenz gewährleisten, um die gesellschaftliche Akzeptanz solcher Kontaktnachverfolgungs-Apps zu fördern.

Zu diesem Zweck sollten die Anbieter von Kontaktnachverfolgungs-Apps folgende Kriterien berücksichtigen:

- Die Verwendung einer solchen App darf nur auf ausschließlich freiwilliger Basis erfolgen. Der Zugang zu gesetzlich garantierten Rechten darf nicht von der Verwendung einer solchen App abhängig gemacht werden. Jeder muss jederzeit die volle Kontrolle über seine Daten haben und sollte frei entscheiden können, ob er eine solche App nutzt oder nicht.

- Es ist davon auszugehen, dass Kontaktnachverfolgungs-Apps ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen bergen und deshalb vor ihrer Einführung die Durchführung einer Datenschutz-Folgenabschätzung notwendig machen.

- Informationen über die räumliche Nähe zwischen den Nutzern einer Kontaktnachverfolgungs-App können eingeholt werden, ohne ihren Standort ausfindig zu machen. Für eine solche App sind Standortdaten nicht erforderlich und sollten daher auch nicht einbezogen werden.
- Wird bei einem Nutzer eine Infektion mit dem SARS-CoV-2-Virus diagnostiziert, sollten nur die Personen informiert werden, mit denen der Nutzer innerhalb der epidemiologisch relevanten Speicherfrist für die Kontaktnachverfolgung in engem Kontakt stand.
- Für den Betrieb dieser Art von Anwendung kann - je nach der gewählten Architektur - die Nutzung eines zentralen Servers erforderlich sein. In einem solchen Fall und im Einklang mit den Grundsätzen der Datenminimierung und des Datenschutzes durch Technik sollten die von dem zentralen Server verarbeiteten Daten auf das absolute Minimum beschränkt sein:
    - Wird bei einem Nutzer eine Infektion mit dem SARS-CoV-2-Virus diagnostiziert, dürfen Informationen über seine früheren engen Kontakte oder die von seiner App gesendeten Kennungen nur mit Zustimmung des Nutzers erhoben werden. Es muss eine Methode festgelegt werden, mit der festgestellt werden kann, dass der Nutzer tatsächlich infiziert ist, ohne seine Identität preiszugeben. Technisch gesehen könnte dies dadurch erreicht werden, dass Kontakte nur nach Intervention einer Gesundheitsfachkraft, z. B. unter Verwendung eines speziellen Einmalcodes, gewarnt werden.
    - Die auf dem zentralen Server gespeicherten Informationen sollten es dem Verantwortlichen weder ermöglichen, Nutzer zu identifizieren, bei denen eine Infektion diagnostiziert wurde oder die mit infizierten Nutzern in Kontakt gekommen sind, noch die Feststellung von Bewegungsmustern ermöglichen, die für die Bestimmung relevanter Kontakte nicht erforderlich sind.
- Apps dieser Art erfordern die Sendung von Daten, die von Geräten anderer Nutzer gelesen werden sowie das Empfangen dieser Sendungen:
    - Es reicht aus, pseudonymisierte Kennungen zwischen den mobilen Geräten der Nutzer (Computer, Tablets, vernetzte Uhren usw.) auszutauschen, z. B. über die BLE-Technologie (Bluetooth Low Energy).
    - Kennungen müssen unter Verwendung kryptografischer Verfahren nach dem Stand der Technik generiert werden.
    - Die Kennungen müssen regelmäßig erneuert werden, um das Risiko einer physischen Verfolgung und von Koppelungsangriffen zu verringern.
- Apps dieser Art müssen gesichert sein, um sichere technische Prozesse zu gewährleisten. Dies schließt insbesondere Folgendes ein:
    - Die App darf den Nutzern keine Informationen übermitteln, die es ihnen ermöglichen, auf die Identität oder die Diagnose anderer Nutzer zu schließen. Der zentrale Server darf weder Nutzer identifizieren noch Informationen über sie ableiten.

Hinweis: Die vorstehenden Grundsätze beziehen sich auf den erklärten Zweck von *Kontaktnachverfolgungs*-Apps und nur auf diesen Zweck, d. h. sie zielen lediglich darauf ab, Personen, die einem Infektionsrisiko ausgesetzt waren, automatisch zu informieren (ohne sie identifizieren zu müssen). Die Betreiber der App und ihre Infrastruktur können von der zuständigen Aufsichtsbehörde

kontrolliert werden. Die vollständige oder teilweise Befolgung dieser Empfehlungen ist nicht unbedingt ausreichend, um die vollständige Einhaltung der Datenschutzbestimmungen zu gewährleisten.

2. Begriffsbestimmungen

Kontakt	Bei einer App zur Kontaktnachverfolgung ist ein Kontakt ein Nutzer, der mit einem als Virusträger bestätigten Nutzer in eine Interaktion involviert war, deren Dauer und Abstand zum infizierten Nutzer auf das Risiko einer erheblichen Exposition gegenüber dem Virus schließen lässt. Parameter für die Dauer der Exposition und den Abstand zwischen den Personen müssen von den Gesundheitsbehörden definiert werden. Sie können in der App voreingestellt werden.
Standortdaten	Standortdaten beziehen sich auf alle in einem elektronischen Kommunikationsnetz oder von einem elektronischen Kommunikationsdienst verarbeitete Daten, aus denen die geografische Position des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes (im Sinne der Richtlinie) hervorgeht, sowie auf Daten aus möglichen anderen Quellen, die sich beziehen auf: - den Breitengrad, Längengrad oder die Höhenlage des Endgeräts, - die Fahrtrichtung des Nutzers oder - den Zeitpunkt, zu dem die Standortinformationen aufgezeichnet wurden.
Interaktion	Bei einer Kontaktnachverfolgungs-App bezeichnet Interaktion den Austausch von Informationen zwischen zwei Geräten, die sich (räumlich und zeitlich) innerhalb der Reichweite der verwendeten Kommunikationstechnologie (z. B. Bluetooth) in unmittelbarer Nähe zueinander befinden. Diese Definition schließt den Standort der beiden an der Interaktion beteiligten Nutzer aus.
Virusträger	Nach diesen Empfehlungen gilt als Virusträger ein Nutzer, der positiv auf das Virus getestet wurde und eine amtliche Diagnose von einem Arzt oder Gesundheitszentrum erhalten hat.
Kontakt–nachverfolgung	Bei Personen, die (nach von Epidemiologen festzulegenden Kriterien) in engem Kontakt mit einer mit dem Virus infizierten Person standen, besteht ein erhebliches Risiko, dass sie ebenfalls infiziert worden sind und ihrerseits andere infizieren können. Die Kontaktnachverfolgung ist eine Methode zur Seuchenbekämpfung, bei der alle Personen ermittelt werden, die sich in unmittelbarer Nähe zu einem Virusträger befanden, um zu prüfen, ob sie infektionsgefährdet sind, und ihnen gegenüber geeignete gesundheitspolizeiliche Maßnahmen zu ergreifen.

3. Allgemeines

GEN-1	Die Anwendung muss ergänzend zu den herkömmlichen Verfahren zur Nachverfolgung von Kontaktpersonen (wie insbesondere Befragungen von infizierten Personen) eingesetzt werden, d. h. sie muss Teil eines umfassenderen Programms für die öffentliche Gesundheit sein. Sie darf nur so lange eingesetzt werden, bis die Zahl der Neuinfektionen mit den Techniken der manuellen Kontaktnachverfolgung allein bewältigt werden kann.
GEN-2	Spätestens wenn die zuständigen Behörden über die „Rückkehr zur Normalität" entscheiden, muss ein Verfahren eingerichtet werden, um die Erfassung der Kennungen zu unterbinden (allgemeine Deaktivierung der Anwendung, Aufforderung zur Deinstallation der Anwendung, automatische Deinstallation usw.) und die Löschung aller erhobenen Daten aus allen Datenbanken (mobile Anwendungen und Server) zu veranlassen.
GEN-3	Der Quellcode der App und ihres „Backends" muss offen sein, und die technischen Spezifikationen müssen veröffentlicht werden, damit jeder Betroffene den Code prüfen und gegebenenfalls zur Verbesserung des Codes, zur Korrektur möglicher Fehler und zur Gewährleistung der Transparenz bei der Verarbeitung personenbezogener Daten beitragen kann.
GEN-4	Die App muss stufenweise eingeführt werden, sodass es möglich ist, ihre Wirksamkeit unter dem Gesichtspunkt der öffentlichen Gesundheit schrittweise zu validieren. Zu diesem Zweck muss im Vorfeld ein Bewertungsprotokoll mit Indikatoren festgelegt werden, mit denen die Wirksamkeit der App gemessen werden kann.

4. Zweck der Anwendung

PUR-1	Die App darf nur dem Zweck dienen, Kontakte nachzuverfolgen, damit Personen, die möglicherweise dem SARS-CoV-2-Virus ausgesetzt sind oder waren, gewarnt und versorgt werden können. Sie darf nicht für andere Zwecke eingesetzt werden.
PUR-2	Die App darf nicht unter Umgehung ihres primären Verwendungszwecks für die Überwachung von Quarantänemaßnahmen oder Ausgangsbeschränkungen und/oder der Einhaltung von Maßnahmen der sozialen Distanzierung eingesetzt werden.
PUR-3	Die App darf nicht dazu verwendet werden, Schlüsse über den Standort der Nutzer auf der Grundlage ihrer Interaktionen und/oder anderer Kriterien zu ziehen.

5. Funktionale Überlegungen

FUNC-1	Die App muss eine Funktion bieten, über die Nutzer informiert werden können, dass sie einem Infektionsrisiko ausgesetzt waren. Diese Information beruht auf

	der räumlichen Nähe zu einem infizierten Nutzer innerhalb eines Zeitfensters von X Tagen vor dem positiven Testergebnis (der Wert X wird von den Gesundheitsbehörden festgelegt).
FUNC-2	Die App sollte Empfehlungen für Nutzer enthalten, bei denen festgestellt wurde, dass sie einem Infektionsrisiko ausgesetzt waren. Sie sollte Anweisungen zu den von den exponierten Nutzern zu befolgenden Maßnahmen weitergeben und ihnen die Möglichkeit bieten, Rat einzuholen. In solchen Fällen sollte zwingend eine Person eingeschaltet werden.
FUNC-3	Der Algorithmus, der das Infektionsrisiko unter Berücksichtigung von Abstands- und Zeitfaktoren misst und somit bestimmt, wann ein Kontakt in die Kontaktnachverfolgungsliste aufzunehmen ist, muss justierbar sein, um die neuesten Erkenntnisse über die Ausbreitung des Virus berücksichtigen zu können.
FUNC-4	Die **Nutzer müssen innerhalb der Inkubationszeit des Virus informiert werden, wenn sie dem Virus ausgesetzt waren**, oder regelmäßig Informationen darüber erhalten, ob sie dem Virus ausgesetzt waren oder nicht.
FUNC-5	Die App sollte mit anderen in den Mitgliedstaaten entwickelten Anwendungen interoperabel sein, damit Nutzer, die in den Mitgliedstaaten auf Reisen sind, effizient benachrichtigt werden können.

6. Daten

DATA-1	Die App muss in der Lage sein, Daten über Nahkommunikationstechnologien wie Bluetooth Low Energy zu senden und zu empfangen, damit Kontakte nachverfolgt werden können.
DATA-2	Die gesendeten Daten müssen kryptographisch starke pseudozufällige Kennungen einschließen, die von der App generiert werden und für sie spezifisch sind.
DATA-3	Das Kollisionsrisiko bei pseudozufälligen Kennungen sollte hinreichend gering sein.
DATA-4	Pseudozufällige Kennungen müssen regelmäßig und so häufig erneuert werden, dass das Risiko einer Re-Identifikation, physischen Verfolgung oder Herstellung einer Verbindung zwischen Einzelpersonen durch andere Personen, einschließlich durch die Betreiber eines zentralen Servers, andere Nutzer oder böswillige Dritten, begrenzt ist. Diese Kennungen müssen von der App des Nutzers – eventuell auf der Grundlage einer vom zentralen Server bereitgestellten Ausgangszahl – generiert werden.
DATA-5	Nach dem Grundsatz der Datenminimierung darf die App keine anderen Daten erheben als die, die für die Nachverfolgung von Kontakten unbedingt erforderlich sind.

DATA-6	Standortdaten dürfen für die Kontaktnachverfolgung nicht erhoben werden. Standortdaten dürfen nur zu dem Zweck verarbeitet werden, die Interaktion der App mit ähnlichen Anwendungen in anderen Ländern zu ermöglichen, und sollten auf das für diesen alleinigen Zweck unbedingt erforderliche Maß beschränkt werden.
DATA-7	Mit der App dürfen über die für die Zwecke der App unbedingt erforderlichen Gesundheitsdaten hinaus keine weiteren Gesundheitsdaten erhoben werden, ausgenommen auf fakultativer Basis und ausschließlich als Entscheidungshilfe im Hinblick auf die Information des Nutzers.
DATA-8	Die Nutzer müssen über alle personenbezogenen Daten, die erhoben werden, informiert werden. Diese Daten dürfen nur mit Genehmigung des Nutzers erhoben werden.

7. Technische Eigenschaften

TECH-1	Die App sollte verfügbare Technologien wie die Nahkommunikationstechnologie (z. B. Bluetooth Low Energy) nutzen, um Nutzer in der Nähe des Geräts, auf dem die App aktiviert ist, zu detektieren.
TECH-2	Die Kontakthistorie eines Nutzers sollte über einen bestimmten vorab festgelegten Zeitraum im Gerät gespeichert werden.
TECH-3	Die App kann zur Implementierung eines Teils ihrer Funktionen auf einen zentralen Server gestützt werden.
TECH-4	Die App muss auf einer Architektur beruhen, die sich so weit wie möglich auf die Geräte der Nutzer stützt.
TECH-5	Auf Veranlassung der Nutzer, die als mit dem Virus infiziert gemeldet wurden und deren Status durch eine entsprechend autorisierte Gesundheitskraft bestätigt wurde, sollte die Kontakthistorie dieser Nutzer oder sollten deren eigene Kennungen dem zentralen Server übermittelt werden.

8. Sicherheit

SEC-1	Der Status der Nutzer, die sich über die App als SARS-CoV-2-positiv melden, muss z. B. durch Bereitstellung eines Einmalcodes, der mit einer Testeinrichtung oder einer Gesundheitsfachkraft verbunden ist, überprüft werden. Kann die Bestätigung nicht auf sichere Weise erlangt werden, dürfen die Daten nicht verarbeitet werden.
SEC-2	Die an den zentralen Server gesendeten Daten müssen über einen sicheren Kanal übermittelt werden. Die Nutzung von Benachrichtigungsdiensten durch OS-Plattformanbieter sollte sorgfältig geprüft werden und darf nicht dazu führen, dass Daten an Dritte weitergegeben werden.
SEC-3	Anfragen müssen so gesichert sein, dass sie nicht durch böswillige Nutzer manipuliert werden können.

SEC-4	Es müssen kryptografische Techniken nach dem Stand der Technik eingesetzt werden, um den Austausch zwischen der App und dem Server sowie zwischen Anwendungen zu sichern und um generell die in den Apps und auf dem Server gespeicherten Informationen zu schützen. Eingesetzt werden können beispielsweise folgende Techniken: Symmetrische und asymmetrische Verschlüsselung, Hash-Funktionen, Protokolle wie Private Membership Test und Private Set Intersection, Bloom-Filter, Private Information Retrieval, homomorphe Verschlüsselung usw.
SEC-5	Der zentrale Server darf keine Verbindungsendpunkt-Identifikatoren (z. B. IP-Adressen) von Nutzern aufbewahren, auch nicht von Nutzern, die positiv diagnostiziert wurden und ihre Kontakthistorie oder ihre eigenen Kennungen übermittelt haben.
SEC-6	Um Identitätsbetrug oder die Erstellung falscher Nutzerprofile zu verhindern, muss die App durch den Server authentifiziert werden.
SEC-7	Der zentrale Server muss seinerseits durch die App authentifiziert werden.
SEC-8	Die Server-Funktionen sollten vor Replay-Angriffen geschützt werden.
SEC-9	Die vom zentralen Server übermittelten Informationen müssen signiert werden, um ihre Herkunft und Integrität zu bestätigen.
SEC-10	Nur befugte Personen dürfen Zugang zu allen auf dem zentralen Server gespeicherten und nicht öffentlich zugänglichen Daten erhalten.
SEC-11	Der Berechtigungsmanager des Geräts auf der Ebene des Betriebssystems darf nur die erforderlichen Berechtigungen für den Zugang zu den Kommunikationsmodulen und deren Nutzung – soweit notwendig – und die Speicherung der Daten im Endgerät sowie für den Austausch von Informationen mit dem zentralen Server anfordern.

9. Schutz der personenbezogenen Daten und der Privatsphäre natürlicher Personen

Hinweis: Die folgenden Empfehlungen *betreffen eine App, deren einziger Zweck die Nachverfolgung von Kontakten ist.*

PRIV-1	Bei einem Austausch von Daten ist die Privatsphäre der Nutzer (und insbesondere der Grundsatz der Datenminimierung) zu achten.
PRIV-2	Die App darf, wenn sie genutzt wird, keine direkte Identifizierung der Nutzer ermöglichen.
PRIV-3	Die App darf keine Nachverfolgung der Nutzerbewegungen ermöglichen.
PRIV-4	Die Nutzer dürfen über die App nichts über andere Nutzer erfahren (vor allem nicht, ob sie Virusträger sind).
PRIV-5	Das Vertrauen in den zentralen Server muss begrenzt sein. Die Verwaltung des zentralen Servers muss klar definierten Governance-Regeln folgen und alle erforderlichen Maßnahmen zur Gewährleistung seiner Sicherheit einschließen. Der Standort des zentralen Servers sollte so gewählt werden, dass eine wirksame Aufsicht durch die zuständige Aufsichtsbehörde gewährleistet ist.
PRIV-6	Es muss eine Datenschutz-Folgenabschätzung durchgeführt werden, die veröffentlicht werden sollte.
PRIV-7	Die App sollte dem Nutzer lediglich Aufschluss darüber geben, ob er dem Virus ausgesetzt war, d. h., wenn möglich ohne Informationen über andere Nutzer, die Häufigkeit und den Zeitpunkt der Exposition.
PRIV-8	Die über die App übermittelten Informationen dürfen den Nutzern weder die Identifizierung von infizierten Nutzern noch die Nachverfolgung des Bewegungsprofils dieser Nutzer ermöglichen.
PRIV-9	Die über die App übermittelten Informationen dürfen den Gesundheitsbehörden die Identifizierung von potenziell infizierten Nutzern nicht ohne deren Einwilligung ermöglichen.
PRIV-10	Anfragen der App an den zentralen Server dürfen keine Hinweise auf den Virusträger enthalten.
PRIV-11	Anfragen der App an den zentralen Server dürfen keine unnötigen Informationen über den Nutzer preisgeben, außer wenn dies in Bezug auf seine pseudonymisierten Kennungen und Kontaktliste notwendig ist.
PRIV-12	Koppelungsangriffe dürfen nicht möglich sein.
PRIV-13	Die Nutzer müssen ihre Rechte mittels der App ausüben können.
PRIV-14	Die Deinstallation der App muss die Löschung aller lokal erhobenen Daten bewirken.
PRIV-15	Die App sollte nur Daten erfassen, die von Instanzen der Anwendung oder interoperablen, gleichwertigen Anwendungen übermittelt werden. Daten, die andere Apps und/oder Nahkommunikationsgeräte betreffen, dürfen nicht erhoben werden.

PRIV-16	Um eine Re-Identifikation durch den zentralen Server zu vermeiden, sollten Proxy-Server eingerichtet werden. Zweck dieser vertrauenswürdigen, d. h. *non-colluding*, Server ist es, die Kennungen mehrerer Nutzer (sowohl von Virusträgern als auch angeforderte Kennungen) zu mischen, bevor sie mit dem zentralen Server geteilt werden, um zu verhindern, dass der zentrale Server Kenntnis von den Identifikatoren (z. B. IP-Adressen) der Nutzer erhält.
PRIV-17	App und Server müssen mit großer Sorgfalt entwickelt und konfiguriert werden, damit keine unnötigen Daten erhoben werden (z. B. sollten keine Kennungen in die Serverprotokolle aufgenommen werden) und um die Verwendung von SDK Dritter zu vermeiden, die Daten für andere Zwecke sammeln.

Die meisten derzeit diskutierten Kontaktnachverfolgungs-Apps folgen im Wesentlichen zwei Ansätzen, wenn ein Nutzer als infiziert bestätigt wird: Sie können entweder eine Liste der erfassten Nahkontakte an einen Server senden, oder sie können die Liste ihrer eigenen ausgesendeten Identifikatoren übermitteln. Die folgenden Grundsätze unterscheiden sich nach diesen beiden Ansätzen. Dass nur diese beiden Ansätze hier erörtert werden, bedeutet nicht, dass andere Vorgehensweisen nicht ebenso möglich oder gar vorzuziehen wären, z. B. Implementierung einer E2E-Verschlüsselung oder anderer Technologien, die die Sicherheit oder den Schutz der Privatsphäre fördern.

9.1. Grundsätze, die nur gelten, wenn die App eine Kontaktliste an den Server sendet:

CON-1	Der zentrale Server muss auf freiwillige Veranlassung der positiv auf SARS- CoV -2 getesteten Nutzer hin ihre Kontakthistorie erfassen.
CON-2	Der zentrale Server darf die Liste pseudonymisierter Kennungen infizierter Nutzer weder aufbewahren noch verbreiten.
CON-3	Die auf dem zentralen Server gespeicherte Kontakthistorie muss gelöscht werden, sobald die Nutzer über ihre Nähe zu einer positiv getesteten Person informiert worden sind.
CON-4	Außer in Fällen, in denen der als Virusträger bestätigte Nutzer seine Kontakthistorie mit dem zentralen Server teilt, dürfen keine Daten vom Gerät des Nutzers abgerufen werden. Gleiches gilt für den Fall, dass der Nutzer den Server auffordert, sein Infektionsrisiko zu ermitteln.
CON-5	Alle in der Kontakthistorie lokal gespeicherte Kennungen müssen X Tage nach ihrer Erfassung gelöscht werden (der Wert X wird von den Gesundheitsbehörden festgelegt).
CON-6	Von verschiedenen Nutzern übermittelte Kontakthistorien dürfen nicht weiterverarbeitet werden, z. B. durch Kreuzkorrelation, um globale Abstandskarten zu erstellen.
CON-7	Die Daten in den Server-Protokollen müssen minimiert werden und den Datenschutzanforderungen entsprechen.

9.2. Grundsätze, die nur gelten, wenn die App eine Liste eigener Kennungen an einen Server sendet:

ID-1	Der zentrale Server muss auf freiwillige Veranlassung eines positiv auf SARS-CoV-2 getesteten Nutzers hin die Kennungen erfassen, die von der App dieses Nutzers gesendet wurden.
ID-2	Der zentrale Server darf die Kontakthistorie der mit dem Virus infizierten Nutzer weder aufbewahren noch verbreiten.
ID-3	Auf dem zentralen Server gespeicherte Kennungen müssen gelöscht werden, sobald sie den anderen Apps übermittelt wurden.
ID-4	Außer in Fällen, in denen der als Virusträger bestätigte Nutzer seine Kennungen mit dem zentralen Server teilt, dürfen keine Daten vom Gerät des Nutzers abgerufen werden. Gleiches gilt für den Fall, dass der Nutzer den Server auffordert, sein Infektionsrisiko zu ermitteln.
ID-5	Die Daten in den Server-Protokollen müssen minimiert werden und den Datenschutzanforderungen entsprechen.